WHAT IS CLAIMED IS:

1. A quantitative competition method for a system in which a plurality of participant devices send their secret aimed values to a server device and said server device determines which of said plurality of participant devices has offered the maximum or minimum one of said aimed values received, said method comprising the steps wherein:

(a) each of said participant devices processes an initial value peculiar to said participant device with a predetermined one-way function by the number of times corresponding to said aimed value to generate aimed value information;

(b) either one of said each participant device and said server device processes said initial value with said one-way function to generate an updated initial value;

(c) said server device makes a check for matching between said updated aimed values and said aimed value information of said participant devices; and

(d) upon first detection of matching in said step (c), said server device decides that said aimed value of that one of said participant devices which corresponds to said updated value having matched said aimed value information is maximum or minimum.

2. The method of claim 1, further comprising a step of repeating the updating of said initial value in said step (b) and the check for matching in said step (c) when no matching is detected in said step (c).

3. The method of claim 2, wherein said step (b) includes a step of generating said updated initial value by said server device.

4. The method of claim 3, wherein: there is provided a conversion

table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values corresponding thereto;

said step (a) includes a step wherein, letting M be the number of participant devices, an m-th participant device m computes said aimed value information by

$$\gamma_m = g(h^{km}(IV_m))$$

where g is a one-way function, IV_m is said initial value, k_m is an index corresponding to said aimed value of said participant device m, and $h^{km}(IV_m)$ indicates that said initial value IV_m is processed with said one-way function h by k_m times;

said step (b) includes a step wherein said server device generates said updated initial value by

$$D_m = g(h^k(IV_m)); \text{ and}$$

said step (c) includes a step of making a check for said aimed value information $\gamma_m = D_m$.

5. The method of claim 2, wherein said step (b) includes a step wherein said each participant device generates said updated value by the number of times requested by said server device and sends said updated initial value to said server device.

6. The method of claim 5, wherein: there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values corresponding thereto; and

said step (a) includes the steps wherein:

(a-1) letting M be the number of participant devices, an m-th participant device m computes said aimed value information by

$\gamma_m = g(h^{km}(IV_m))$

where g is a one-way function, IV_m is said initial value, k_m is an index corresponding to said aimed value of said participant device m, and $h^{km}(IV_m)$ indicates that said initial value IV_m is processed with said one-way function h by k_m times;

(a-2) said each participant device generates verification information $C_m = h^{K+1}(IV_m)$ and sends it to said server device together with said aimed value information γ_m; and

(a-3) said server device publishes said aimed value information γ_m and said verification information $C_m = h^{K+1}(IV_m)$ received from said each participant device on a bulleting board accessible from all of said participant devices.

7. The method of claim 6, wherein: said step (b) includes the steps wherein:

(b-1) said server device requests said each participant device to send $D_m = h^k(IV_m)$ corresponding to said index k; and

(b-2) said each participant device responds to the request of said server device to generate $D_m = h^k(IV_m)$ corresponding to said index k as said updated initial value and sends it to said server; and

said step (c) includes a step of generating $g(D_m)$ and making a check for said aimed value information $\gamma_m = g(D_m)$.

8. The method of claim 7, wherein: said step (b) includes a step (b-0) wherein said server device sets said index k to an upper limit value K; and

said step (c) includes the steps wherein said server device:

(c-1) publishes said $D_m = h^k(IV_m)$ received from said each participant device on said bulletin board;

(c-2) computes said $g(D_m)$ for said each participant device m;

(c-3) makes a check to see if said $g(D_m)$ matches said aimed value information;

(c-4) if no match is detect for any of said m in said step (c-3), replaces said D_m with said C_m, decrementing said index k by one and returns to said step (b-1); and

(c-5) if a match is detected in said step (c-3), determines that the value corresponding to said index k at that time is said maximum or minimum aimed value.

9. The method of claim 8, wherein said step (c-1) includes a step wherein said server device generates $h(D_m)$ and makes a check to see if $h(D_m) = C_m$ holds.

10. The method of claim 8, wherein said step (c-5) includes a step wherein said server device publishes said determined maximum or minimum aimed value and said $h^{km}(IV_m)$ on said bulletin board.

11. The method of claim 5, wherein: there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values corresponding thereto; and

said step (a) includes the steps wherein:

(a-1) letting M be the number of participant devices, an m-th participant device m computes said aimed value information by

$$\gamma_m = g(h^{km}(IV_m))$$

where g is a one-way function, IV_m is said initial value, k_m is an index corresponding to said aimed value of said participant device m, and $h^{km}(IV_m)$ indicates that said initial value IV_m is processed with said one-way function h by k_m times;

(a-2) said each participant device generates verification information

$C_m = h^{K+1}(IV_m)$ and sends it to said server device together with said aimed value information γ_m; and

(a-3) said server device publishes said aimed value information γ_m and said verification information $C_m = h^{K+1}(IV_m)$ received from said each participant device on a bulleting board accessible from all of said participant devices;

said step (b) includes the steps wherein: said server device:

(b-0) said server device sets said index k to an upper limit value K;

(b-1) said server device inquires said each participant device m about whether said aimed value information corresponds to said index;

(b-2) said server device checks whether an answer from said each participant device acknowledges said correspondence;

(b-3) if said answer from said each participant device denies said correspondence, said server device decrements said k by one and returns to said step (b-1);

(b-4) if said answer from said each participant device acknowledges said correspondence, said server device requests said each participant device to present an updated initial value $h^k(IV_m)$;

(b-5) said each participant device generates $D_m = h^k(IV_m)$ using said initial value IV_m of its own and sends said D_m to said server device; and

(b-6) said server device publishes said D_m from said each participant device on said bulletin board; and

said step (c) includes the steps wherein said server device:

(c-1) generates $h(D_m)$'s for all of said D_m's received from all of said participant devices;

(c-2) checks whether said $h(D_m)$'s match said verification information C_m's on said bulletin board, respectively;

(c-3) if no mismatch is detected in said step (c-1), generates $g(D_j)$ for D_j presented by a participant device j having bid;

(c-4) checks whether said $g(D_j)$ matches said aimed value information γ_j of said participant device j on said bulletin board; and

(c-5) if said $g(D_j)$ matches said γ_j in said step (c-4), decides that said participant device j sent to said server device said aimed value information corresponding to said aimed value k.

12. The method of claim 1, wherein: there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values corresponding thereto; and

said step (a) includes the steps wherein:

(a-1) letting M be the number of participant devices, an m-th participant device m computes said aimed value information by

$$\gamma_m = g(h^{km}(IV_m))$$

where g is a one-way function, IV_m is said initial value, k_m is an index corresponding to said aimed value of said participant device m, and $h^{km}(IV_m)$ indicates that said initial value IV_m is processed with said one-way function h by k_m times;

(a-2) said each participant device generates verification information $C_m = h^{K+1}(IV_m)$;

(a-3) said each participant device m generates $h(PR_m(+)R_m)$ from a random number R_m and said aimed value PR_m and sends said $h(PR_m(+)R_m)$ to said server device together with said γ_m and said C_m, said (+) represents a predetermined arbitrary operation;

said step (b) includes the steps wherein:

(b-1) said server device publishes its received γ_m, $h(PR_m(+)R_m)$ and

ID_m on said bulletin board;

(b-2) said server device requests said each participant device to present said aimed value PR_m and said random number R_m;

(b-3) said each participant device sends said aimed value PR_m and said random number R_m to said server device;

(b-4) said server device determines from its received PR_m and R_m an index k corresponding to the maximum one of said aimed values and a participant device j having sent said aimed value information corresponding to said index k;

(b-5) said server device request all of said participant devices to present $h^k(IV_m)$; and

(b-6) said each participant device generates $D_m=h^k(IV_m)$ as said updated initial value using the initial value IV_m of its own, and sends said $D_m=h^k(IV_m)$ to said server device;

said step (c) includes the steps wherein said server device:

(c-1) publishes all of its received D_m's on said bulletin board;

(c-2) generating $h(D_m)$'s for all of said D_m's;

(c-3) checks whether said $h(D_m)$'s match said verification information C_m's on said bulletin board, respectively;

(c-4) if no mismatch is detected in said step (c-3), generates $g(D_j)$ for D_j presented by said participant device j having sent said maximum aimed value determined in said step (b-4); and

(c-5) checks whether said $g(D_j)$ matches said aimed value information γ_j of said participant device j on said bulletin board; and

said step (d) includes a step wherein if a match is detected in said step (c-5), said server device decides that said participant device j sent said aimed value information for said aimed value k.

13. The method of claim 12, wherein said step (d) includes the steps of:

(d-1) generating $E_m = g(h^{t-k}(h^k(IV_m))$ for t such that $k \leq t \leq K$ and for all of said m's except said j;

(d-2) checking whether these E_m's match said aimed value information γ_m on said bulletin board; and

(d-3) if no match is detected in said step (d-2), deciding that said k is an index corresponding to the maximum or minimum aimed value, and outputting said k and said identifier ID_m of said participant device j having presented said aimed value.

14. The method of claim 12 or 13, wherein: said each participant device m adds to the computation using said aimed value PR_m and said random number R_m in said step (a-3) additional information I_m about said aimed value information by said each participant device m, and outputs $h(PR_m(+)I_m(+)R_m)$; and

in said step (b-2) said server device requests all of said participant devices to present said additional information I_m as well as said aimed value PR_m and said random number R_m.

15. The method of claim 1, wherein: there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto;

said step (a) includes the steps wherein:

(a-1) each said bidding device generates $h(H_m^{(K)})$ as aimed value information of said each participant device by repeating, for each of a sequence of index values k from at least k_m corresponding to an aimed value of said each participant device to an upper limit index value K, processing of:

combining an initial value of said each participant device with select information to provide combined information and

operating a one-way function h on said combined information to generate an updated value, said select information indicating whether said each index value k is an aimed value or not; and

sends said aimed value information $H_m^{(K)}$ to said server device;

(a-2) said server device publishes said received aimed value information $H_m^{(K)}$ on a bulletin board accessible from all of said participant devices;

said step (b) includes the steps wherein:

(b-1) said server device requests said each participant device to send an updated initial value $\{H_m^{(k-1)}, b_m^{(k)}\}$ corresponding to each value of said index k in the descending order from K; and

(b-2) said each participant device generates and sends $\{H_m^{(k-1)}, b_m^{(k)}\}$ as said updated initial value to said server device;

said step (c) includes the steps wherein said server device:

(c-1) publishes on said bulletin board said updated initial value $\{H_m^{(k-1)}, b_m^{(k)}\}$ received from said each participant device;

(c-2) processes said updated initial value $H_m^{(k)}$ with a one-way function h to generate $H_m^{(k)} = h(H_m^{(k-1)}||b_m^{(k)})$;

(c-3) checks whether said updated initial value $H_m^{(k)}$ matches $H_m^{(k)}$ received previously; and

(c-4) if a match is detected in said step (c-3), decides whether said select information $b_m^{(k)}$ represents that the corresponding index k is the index k_m of said aimed value; and

said step (d) is a step wherein if the result of decision in said step (c-4) is true, said server device outputs said index concerned and the corresponding

participant device number m, and if the result of decision is false, said server device returns to said step (b) and repeats processing for the next index value k.

16. The method of claim 1, wherein: there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto;

said step (a) includes the steps wherein:

(a-1) upon each processing of said initial value with said one-way function h, said each participant device generates an updated initial value by adding said processed initial value with select information $b_m^{(k)}$ indicating whether said processed initial value is an aimed value for one value of said index k, and generates $H_m^{(k)}$ by repeatedly performing this processing from at least that index k_m of a sequence of indexes which corresponds to said aimed value to the upper limit value K, and sends said $H_m^{(k)}$ as said aimed value information to said server device;

(a-2) said server device publishes its received aimed value information $H_m^{(K)}$ on a bulletin board accessible from all of said participant devices;

said step (b) includes the steps wherein:

(b-1) for each value of said index k in descending order from K, said server device inquires said each participant device about whether it has bid for said index k, and said each participant device responds YES or NO to said inquiry;

(b-2) upon first detection of the response YES, said server device requests said each participant device to send its updated initial value $H_m^{(k-1)}$; and

(b-3) said each participant device generates and sends ($H_m^{(k-1)} = h(H_m^{(k-}$

$^{2)}$|| $b_m^{(k-1)}$) as said updated initial value to said server device;

said step (c) includes the steps wherein said server device:

(c-1) publishes on said bulletin board said updated initial value ($H_m^{(k-1)}$) received from said each participant device;

(c-2) letting a and $\underline{a}$ represent predetermined values of said select information $b_m^{(k)}$ indicating bidding and not bidding, respectively, generate, for said participant device m having bid for the current index k,

$$H_m = h(\ldots h(h(H_m^{(k-1)} || a) || \underline{a}) \ldots || \underline{a})$$

through the use of said updated initial value $H_m^{(k-1)}$, and for every one of the other participant devices m, generate

$$H_m = h(\ldots h(h(H_m^{(k-1)} || a) || \underline{a}) \ldots || \underline{a})$$

through the use of said updated initial values $H_m^{(k-1)}$;

(c-3) checks whether said H_m for said each participant device matches said $H_m^{(k)}$ published on said bulletin board; and

(c-4) if a match is detected in said step (c-3), determines that said participant device having responded YES is the winning bidding device, and publishes the current value of said index k as the index K_m of the aimed value of said winning bidding device.

17. The method of claim 1, wherein: there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, and let the initial value of said each participant device be represented by IV_m, where m = 1, 2, ..., M, M being an integer equal to or greater than 2;

said step (a) is a step wherein said each participant device generates $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ using a predetermined positive integer x_m, said initial value IV_m and one-way functions h and g, and sends said $H_m^{(K)}$ as said aimed

value information to said server device;

said step (b) includes the steps wherein:

(b-1) said server device publishes said aimed value information A_m on a bulletin board accessible from all of said participant devices;

(b-2) said server device sends said index k to said each participant device to ask for its updated initial value;

(b-3) said each participant device decides whether its received index k is the index k_m corresponding to said aimed value;

(b-4) if the result of decision in step (b-3) is $k = k_m$, said each participant device generates and sends $H_m^{(k-1)} = g^{xm-1}(IV_m)$ as said updated initial value to said server device; and

(b-5) if the result of decision in said step (b-3) is not $k = k_m$, said each participant device generates and sends $H_m^{(k-1)} = h^{k-km-1}(g^{xm}(IV_m))$ as said updated initial value to said server device;

said step (c) includes the steps wherein said server device:

(c-1) processes said updated initial value $H_m^{(k-1)}$ with said one-way function h to generate $h(H_m^{(k-1)})$;

(c-2) decides whether said $h(H_m^{(k-1)})$ is equal to said aimed value information $H_m^{(K)}$;

(c-3) if it is decided in said step (c-2) that they are equal, updates said aimed value information $H_m^{(K)}$ with said updated initial value $H_m^{(k-1)}$, then decrements said index k by one and return to said step (b-2);

(c-4) if it is decided in said step (c-2) that they are not equal, processes said updated initial value $H_m^{(k-1)}$ with said one-way function g to generate $g(H_m^{(k-1)})$; and

(c-5) decides whether said $g(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$; and

said step (d) is a step wherein if a match is detected in said step (c-5), decides that the aimed value of said participant device corresponding to m and k having provided said match is the maximum or minimum.

18. The method of claim 1, wherein: there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto;

said step (a) includes the steps wherein:

(a-1), letting the initial value of said each participant device be represented by IV_m, where m = 1, 2, ..., M, M being an integer equal to or greater than 2, said each participant device generates $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ using a predetermined positive integer x_m, said initial value IV_m and one-way functions h and g, and sends said H_m as said aimed value information to said server device; and

(a-2) said server device publishes its received aimed value information $H_m^{(K)}$ on a bulletin board accessible from all of said participant devices;

said step (b) includes the steps wherein:

(b-1) for each value of said index k in descending order from K, said server device inquires said each participant device about whether it has bid for said index k, and said each participant device responds YES or NO to said inquiry;

(b-2) upon first detection of the response YES, said server device requests said each participant device to send its updated initial value $H_m^{(k-1)}$;

(b-3) said each participant device decides whether its received k is the index k corresponding to said aimed value;

(b-4) if the result of decision in said step (b-3) is $k = k_m$, said each participant generates and sends $H_m^{(k-1)} = g^{xm-1}(IV_m)$ as said updated initial

value to said server device; and

(b-5) if the result of decision in said step (b-3) is not $k = k_m$, said each participant device generates and sends $H_m^{(k-1)} = g^{xm-1}(IV_m)$ as said updated initial value to said server device; and

said step (c) includes the steps wherein said server device:

(c-1) for said updated initial value $H_m^{(k-1)}$ received from said participant device having responded YES, generates

$$H_m = h^{K-km}g(H_m^{(k-1)})$$

and for said updated initial value received from said each participant device having responded NO, generates

$$H_m = h^{K+1-k}g(H_m^{(k-1)})$$

(c-2) checks whether all of said H_m are equal to said aimed value information $H_m^{(K)}$ published on said bulletin board; and

(c-3) if it is decided in said step (c-2) that they are equal, determines that said participant device having responded YES is the winning bidding device, and publishes the current value of said index k as the index k of the aimed value of said winning bidding device.

19. The method of claim 1, wherein: there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, and let the initial value of said each participant device be represented by IV_m, where $m = 1, 2, \ldots, M$, M being an integer equal to or greater than 2;

said step (a) is a step wherein said each participant device generates $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ using a predetermined positive integer x_m, said initial value IV_m and one-way functions h and g, and sends said $H_m^{(K)}$ as said aimed value information to said server device;

said step (b) includes the steps wherein:

(b-1) said server device publishes said aimed value information $H_m^{(K)}$ on a bulletin board accessible from all of said participant devices;

(b-2) said server device sends said index k to said each participant device to ask for its updated initial value;

(b-3) said each participant device decides whether its received index k is the index k_m corresponding to said aimed value;

(b-4) if the result of decision in step (b-3) is $k = k_m$, said each participant device generates and $H_m^{(k-1)} = g^{xm-1}(IV_m)$ as said updated initial value and sends it to said server device together with a flag indicating that said k and k_m are equal; and

(b-5) if the result of decision in said step (b-3) is not $k = k_m$, said each participant device generates and sends $H_m^{(k-1)} = h^{k-km-1}(g^{xm}(IV_m))$ as said updated initial value to said server device;

said step (c) includes the steps wherein said server device:

(c-1) checks whether its received updated initial value $H_m^{(k-1)}$ is added with said flag;

(c-2) if it is decided in said step (c-1) that said flag is added, processes said updated initial value $H_m^{(k-1)}$ with said one-way function g to generate $g(H_m^{(k-1)})$;

(c-3) decides whether said $g(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$;

(c-4) if it is decided in said step (c-1) that no flag is added, processes said updated initial value $H_m^{(k-1)}$ with said one-way function h to generate $h(H_m^{(k-1)})$;

(c-5) decides whether said $h(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$;

(c-6) if it is decided in said step that they are equal, updates said aimed value information $H_m^{(K)}$ with said initial value $H_m^{(k-1)}$, then decrements said index k by one and return to said step (b-2); and

(c-7) if it is decided in said step (c-5), processes said initial value $H_m^{(k-1)}$ with said one-way function g to generate $g(H_m^{(k-1)})$ and returns to said step (c-3); and

said step (d) is a step wherein if a match is detected in said step (c-3), decides that the aimed value of said participant device corresponding to m and k having provided said match is the maximum or minimum.

20. A quantitative competition method for a system in which a plurality of participant devices send their secret aimed values to a server device and said server device determines which of said plurality of participant devices has offered the maximum or minimum one of said aimed values received, and in which there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, and m = 1, 2, ..., M, M being an integer equal to or greater than 2; said method comprising the steps wherein:

(a) each of said participant devices processes, with a predetermined one-way function h and through the use of said conversion table, information $k(+)b_m^{(k)}(+)R_m^{(k)}$, which contains each index k equal to or larger than an index k_m corresponding to said aimed value, select information $b_m^{(k)}$ indicating whether said index k corresponds to said aimed value, and a random number $R_m^{(k)}$, to generate at least $K-k_m+1$ pieces of aimed value information $h(k(+)b_m^{(k)}(+)R_m^{(k)})$, and sends these pieces of aimed value information to said server device, A(+)B representing a predetermined arbitrary operation;

(b) said server device publishes its received aimed value information

on a bulletin board accessible from all of said participant devices;

(c) said server device obtains said random number R_m corresponding to each of said sequence of indexes k;

(d) letting a be a predetermined value with which said select information $b_m^{(k)}$ indicates said aimed value, said server device calculates $h(k(+)a(+)R_m^{(k)})$;

(e) said server device checks said aimed values on said bulletin board for matching with said calculated $h(k(+)a(+)R_m^{(k)})$; and

(f) if a match is detected in said step (e), said server device decides that the aimed value of the aimed value information of a participant device having sent said random number $R_m^{(k)}$ at that time is the maximum or minimum value.

21. The method of claim 20, further comprising a step wherein if a match is detected in said step (d), said server device repeats said steps (c), (d) and (e) for the next value of said index k.

22. The method of claim 21, wherein said step (c) includes the steps wherein: said server device requests said each participant device to send said random number $R_m^{(k)}$ corresponding to said index k; said each participant device sends said requested random number $R_m^{(k)}$ to said server device; and said server device receives said random number $R_m^{(k)}$.

23. The method of claim 21, wherein:

said step (a) includes a step wherein said each participant device sends said aimed value information $h(k(+)b_m^{(k)}(+)R_m^{(k)})$ to said server device together with said random number $R_m^{(k)}$;

said step (b) includes a step wherein said server device stores said random number $R_m^{(k)}$ in a nonpublic memory; and

said step (c) includes the steps wherein: said server device requests

said each participant device to send said random number $R_m^{(k)}$ corresponding to said index k; said each participant device sends said requested random number $R_m^{(k)}$ to said server device; and said server device receives said random number $R_m^{(k)}$.

24. The method of claim 4, 12, 15, 16, 17, 18, 19 or 20 wherein said sequences of indexes k and values selectable as said aimed values are both monotonous increasing values in the same direction, and in said step (c) said server device determines the maximum aimed value.

25. The method of claim 4, 12, 15, 16, 17, 18, 19 or 20, wherein said sequences of indexes k and values selectable as said aimed values are both monotonous increasing values in opposite directions, and in said step (c) said server device determines the minimum aimed value.

26. The method of claim 4, 12, 15, 16, 17, 18, 19 or 20, wherein let an arbitrary aimed value be represented by PR = F(k)+Q, where F(k) is a value in said conversion table corresponding to said index k and Q is a fraction which is a positive integer which satisfies $F(k+1)-F(k)>Q\geq 0$;

said step (a) includes a step wherein, letting said aimed value PR_m of said each participant device m be represented by $PR_m = F(k_m)+Q_m$, said each participant device m generates said aimed value information by processing said initial value with said one-way function h by the number of times corresponding to k_m, sends said aimed value information to said server device together with said fraction Q_m, where m = 1, 2, ..., M, M being an integer equal to or greater than 2;

said step (b) includes a step wherein said server device publishes said aimed value information and said fraction Q_m on a bulletin board accessible from all of said participant devices;

said step (c) includes a step where said server device makes a check

for matching between said updated initial value and said aimed value information for each index value in an ascending or descending order of said fraction Q_m where m = 1, 2, ..., M; and

said step (d) includes a step wherein upon first detection of a match in said step (c), said server device finishes said check and determines, from k_m and m at the time of detecting the match, that $PR_m = F(k_m)+Q_m$ is said maximum or minimum aimed value.

27. The method of claim 1, 4, 12, 15, 16, 17, 18, 19 or 20, further comprising the steps wherein:

(0-1) said each participant device m sends its identifier ID_m to a provisional identifier registration device;

(0-2) said provisional identifier registration device issues a provisional identifier AID_m for said identifier ID_m, and stores said identifier ID_m and said provisional identifier AID_m in pair form in storage means;

(0-3) said provisional identifier registration device sends said provisional identifier AID_m to said each participant device; and

(0-4) said each participant device m sends said provisional identifier AID_m as said identifier to said server device, together with said aimed value information.

28. A participant device for a system in which M participant devices send their aimed values to a server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received, said participant device comprising:

aimed value generating means;

aimed value transforming means which processes said aimed value with a predetermined one-way function by the number of times corresponding

to said aimed value to obtain aimed value information; and

sending means for sending to said server device said aimed value information and an identifier specifying said participant device.

29. The participant device of claim 28, wherein said aimed value transforming means comprises:

a conversion table for converting said aimed value PR_m to the corresponding index k_m;

a one-way function h processor which processes an initial value IV_m inherent to said participant device with a one-way function h by the number of times corresponding to said index k_m to obtain an output $h^{km}(IV_m)$; and

a one-way function g processor which processes said output from said one-way function h processor with a one-way function g to obtain said aimed value information.

30. The participant device of claim 29, further comprising verification information generating means which generates $C_m = h^{K+1}(IV_m)$ as verification information by processing said initial value IV_m with said one-way function h K+1 times and sends said verification information C_m to said server device.

31. The participant device of claim 28, wherein said aimed value information transforming means comprises:

a memory in which there is stored a conversion table which defines the relationships between a sequence of monotone varying values selectable as aimed values and a sequence of indexes, for converting said aimed value PR_m to the corresponding index k_m;

a one-way function h processor which processes an initial value inherent to said participant device with a one-way function h by the number of time corresponding to said index k_m and outputs $h^{km}(IV_m)$; and

a one-way function g processor which processes the output from said

one-way function h processor with a one-way function g to obtain said aimed value information.

32. The participant device of claim 28, which further comprises: a random generator for generating a random number R_m; an operating device for operating said random number R_m and said aimed value PR_m to obtain $PR_m(+)R_m$; one-way function h processing means for processing said $PR_m(+)R_m$ with a one-way function h to obtain $h(PR_m(+)R_m)$; and verification information generating means for processing said initial value IV_m with said one-way function h K+1 times to generate $C_m = h^{K+1}(IV_m)$; and wherein said $h(PR_m(+)R_m)$ and said verification information are sent to said server device together with said aimed value information.

33. The participant device of claim 28, wherein said aimed value transformer comprises:

a conversion table memory which has stored therein a conversion table which defines indexes k = 1, 2, ..., K corresponding to K kinds of values selectable as aimed values;

a select information generator which generates select information $b_m^{(k)}$ indicating whether to select an aimed value corresponding to each of said indexes k = 1, 2, ..., K;

a random generator which generates a random number $R_m^{(k)}$ inherent to said participant device m and said index k;

an operating device which receives said index k, said random number $R_m^{(k)}$ and said select information $b_m^{(k)}$ and performs an operation $k(+)b_m^{(k)}(+)R_m^{(k)}$;

a one-way function h processor which processes said $k(+)b_m^{(k)}(+)R_m^{(k)}$ with a one-way function h to obtain $h(k(+)b_m^{(k)}(+)R_m^{(k)})$; and

a control device which computes said $h(k(+)b_m^{(k)}(+)R_m^{(k)})$ for each of

said indexes k and provides the k pieces information as said aimed value information.

34. The participant device of claim 28, wherein said aimed value transformer comprises:

a conversion table memory which has stored therein a conversion table which defines indexes k = 1, 2, ..., K corresponding to K kinds of values selectable as aimed values, for converting said aimed value PR_m to the corresponding index k_m;

initial value updating means which, for each index k, processes an initial value with a one-way function h and adds the processed initial value with select information $b_m^{(k)}$ for said index k to obtain an updated initial value and repeats this processing until k = K is reached, thereby generating $H_m^{(K)}$;

select information generator which generates said select information $b_m^{(k)}$ whether said aimed value corresponds to each index k from at least k_m to K;

a one-way function h processor which processes said initial value with said one-way function h;

a concatenator which concatenates said $H_m^{(k-1)}$ and said select information to generate $H_m^{\ k} = h(H_m^{(k-1)}||b_m^{(k)})$;

a buffer which temporarily holds the output from said concatenator and outputs said output for the next value of said index k; and

a storage part which, for each value of said index k, stores $H_m^{(k)}$ corresponding thereto; and

wherein said sending means is a means which responds to a request of said server device for said index k to read out $H_m^{(k)}$ from said storage part and send said $H_m^{(k)}$ to said server device.

35. The participant device of claim 28, wherein said aimed value

transformer comprises:

a conversion table memory which has stored therein a conversion table which defines indexes k = 1, 2, ..., K corresponding to K kinds of values selectable as aimed values, for converting said aimed value PR_m to the corresponding index k_m;

a one-way function g processor which processes said initial value IV_m with a one-way function g by a predetermined number of times x_m to generate $g^{xm}(IV_m)$;

a one-way function h processor which processes said $g^{xm}(IV_m)$ with a one-way function h K-k_m times to generate $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ as said aimed value information; and

response generating means which responds to a request from said server device for k to decide whether $k=k_m$, and if true, generates $H_m^{(k-1)} = h^{k-km-1}(g^{xm}(IV_m))$, and if false, generates $H_m^{(k-1)} = g^{xm-1}(IV_m)$; and

wherein said sending means sends said $H_m^{(k-1)}$ in response to said request from said server device for said k.

36. The participant device of claim 28, wherein said aimed value transformer comprises:

a conversion table memory which has stored therein a conversion table which defines the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, for converting said aimed value PR_m to the corresponding index k_m;

a fraction calculating part which, letting an arbitrary aimed value PR be represented by PR = F(k)+Q, where F(k) is a value in said conversion table corresponding to said k and Q is a fraction which is a positive integer which satisfies $F(k+1)-F(k)>Q\geq 0$, calculates said fraction $Q_m = PR_m-F(k_m)$ based on

$F(k_m)$ obtained from said conversion table and said aimed value PR_m; and

a one-way function h processor which processes said initial value IV_m with said one-way function h by the number of times corresponding to said k_m to generate said aimed value information; and

wherein said sending means sends said fraction Q_m to said server device together with said aimed value information.

37. A server device for a system in which M participant devices send their aimed values to said server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received, said device comprising:

a conversion table memory which has stored therein a conversion table which defines the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, for converting said aimed value PR_m to the corresponding index k_m;

a bulletin board on which said server device writes said aimed value information an identifier received from each of said participant devices;

updated initial value generating means which generates an updated initial value by processing said initial value with a one-way function repeatedly in correspondence with values of an index k which is a predetermined consecutive positive integers;

a counter which updates said index k one by one; and

control means which, upon each updating of said index k, compares said updated initial value with said aimed value information on said bulletin board to check whether they match, and determines m and k at the time of first detection of a match.

38. The server device of claim 37, wherein: there are published on said

bulletin board $\gamma_m = g(h^{km}(IV_m))$ as said aimed value information;

said updated initial value generating means includes a one-way function g processor by which a response $D_m = h^k(IV_m)$ received from said participant device in correspondence with said index k is processed with a one-way function g to generate $g(D_m)$ as said updated initial value; and

said control means makes a check to see if there exists on said bulleting board said aimed value information γ_m which matches said updated initial value $g(D_m)$.

39. The server device of claim 38, wherein there is published on said bulletin board $C_m = h^{K+1}(IV_m)$ received from said participant device in advance, said server device further comprising a one-way function h processor which processes said response D_m with a one-way function h to generate $h(D_m)$, and

wherein said control means checks whether $C_m = h(D_m)$ holds, and if not, rewrites said C_m with said D_m and updates said index k on said counter.

40. The server device of claim 37, wherein:

there are published on said bulletin board $C_m = h^{K+1}(IV_m)$, said aimed value information $\gamma_m = h^k(IV_m)$ and $h(PR_m(+)R_m)$ received from said each participant device, said PR_m and said R_m being an aimed value and a random number of said each participant device m;

said control means decides the maximum or minimum aimed value from said aimed values PR_m and said random numbers R_m received from said participant devices, and determines the index k_{mx} corresponding to said maximum or minimum aimed value and requests said each participant device to send $D_m = h^{kmx}(IV_m)$ corresponding to said index k_{mx};

said updated initial value generating means comprises a one-way function h processor for processing D_m with a one-way function h to generate

$h^{K+1-kmx}(D_m)$, and a one-way function g processor for processing D_j with a one-way function g to generate $g(D_j)$; and

said control means makes a check to see if said $h^{K+1-kmx}(D_m)$ matches C_m on said bulletin board and if said $g(D_j)$ matches said γ_m on said bulleting board;

41. The server device of claim 37, wherein:

there are published on said bulletin board $h(k(+)b_m^{(k)}(+)R_m^{(k)})$ together with said aimed value information γ_m received from said each participant device, said $b_m^{(k)}$ being select information whether said index k corresponds to its aimed value and said $R_m^{(k)}$ being a random number generated for said index k;

said server device further comprises an operator for operating $k(+)b(+)R_m^{(k)}$, and a one-way function h processor for processing the result of said operation with a one-way function h to generate $h(k(+)b(+)R_m^{(k)})$, where b is a predetermined value which indicates that said select information $b_m^{(k)}$ has selected the aimed value corresponding to said index k; and

said control means makes a check for matching between said $h(k(+)b(+)R_m^{(k)})$ and said $h(k(+)b_m^{(k)}(+)R_m^{(k)})$ on said bulletin board.

42. The server device of claim 37, wherein:

there is published on said bulletin board, as said aimed value information, $H_m^{(K)}$ generated by said each participant device which, upon each processing of said initial value with a one-way function h, added the processed value with select information $b_m^{(k)}$ indicating whether said value was an aimed value for each value of said index k and repeated this processing from at least the index k_m corresponding to said aimed value to the upper limit value K of said index k;

said updated initial value generating means includes a one-way

function h processor by which $\{H_m^{(k-1)}, b_m\}$ received from said each participant device in answer to an inquiry for said index k is processed with a one-y function h to generate $H_m^{(k)} = h(H_m^{(k-1)} || b_m^{(k)})$; and

said server device includes an updated initial value comparator for making a check to see if said $H_m^{(k)}$ matches previously received $H_m^{(k)}$.

43. The server device of claim 37, wherein: letting an arbitrary aimed value PR be represented by PR = F(k)+Q, where F(k) is a value in said conversion table corresponding to said index k and Q is a fraction which is a positive integer which satisfies $F(k+1)-F(k)>Q\geq 0$, there is published on said bulletin board said fraction Q received from said each participant device, together with said aimed value information;

said server device includes a sequencer for deciding the sequence of said fractions Q_m on said bulletin board;

said updated initial value generating means includes a one-way function h processor for processing said initial value with a one-way function h by k times to generate $h^k(IV_m)$ and a one-way function g processor for processing said $h^k(IV_m)$ with a one-way function g to generate $D_m = g(h^k(IV_m))$; and

control means makes a check to see if said D_m matches said aimed value information on said bulletin board in the sequence of said fractions Q_m.

44. The server device of claim 37, wherein there is published on said bulletin board $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ as said aimed value information received from said each participant device, which further comprises a one-way function h processor by which $H_m^{(k-1)}$ received from said each participant device as an answer to an inquiry for said k is processed with a one-way function h to generate $h(H_m^{(k-1)})$, and a one-way function g processor for processing said answer $H_m^{(k-1)}$ with a one-way function g to generate $g(H_m^{(k-}$

$^{1)}$); and

wherein said control means: makes a check to see if said $h(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$ published on said bulletin board; if a match is detected, updates said aimed value information $H_m^{(K)}$ with said $H_m^{(k-1)}$ and decrements said index k on said counter by one; and if a mismatch is detected, makes a check to see if said $g(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$; and if a match is detected, determines, based on k and m at that time, the maximum or minimum aimed value PR_m and the participant device m having offered said value PR_m.

45. The server device of claims 37, 38, 40, 41, 42, 43 or 44, wherein: letting an arbitrary aimed value PR be represented by PR = F(k)+Q, where F(k) is a value in said conversion table corresponding to said index k and Q is a fraction which is a positive integer which satisfies $F(k+1)-F(k)>Q\geq 0$, there is published on said bulletin board said fraction Q received from said each participant device, together with said aimed value information;

said server device includes:

a sequencer for deciding the sequence of said fractions Q_m on said bulletin board; and

select information comparator for checking whether said select information $b_m^{(k)}$ is equal to a value b indicating the selection of the aimed value corresponding to said index k in said decided sequence of fractions Q_m.

46. The device of claim 29, 31, 33, 34, 36, 37, 40, 41, 43 or 44, wherein said sequence of index values k and said sequence of values selectable as said aimed values on said conversion table are monotone increasing values in the same direction, and said server device determines the maximum aimed value.

47. The device of claim 29, 31, 33, 34, 36, 37, 40, 41, 43 or 44,

wherein said sequence of index values k and said sequence of values selectable as said aimed values on said conversion table are monotone increasing values in opposite directions, and said server device determines the minimum aimed value.

48. A recording medium on which there is recorded as a program the procedure which is followed by an m-th one of M participant devices, where m = 1, 2, ..., M, in a quantitative competition method for a system in which said M participant devices send their aimed values to a server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps of:

(a) processing an initial value inherent to said participant device m with a predetermined one-way function by the number of times corresponding to said aimed value to generate aimed value information

$$\gamma_m = g(h^{km}(IV_m))$$

where g is a one-way function, IV_m is said initial value, k_m is an index corresponding to the aimed value of said participant device m and $h^{km}(IV_m)$ indicates processing of said initial value IV_m with a one-way function h by k_m times; and

(b) sending said aimed value information $\gamma_m = g(h^{km}(IV_m))$ to said server device.

49. A recording medium on which there is recorded as a program the procedure which is followed by an m-th one of M participant devices, where

m = 1, 2, ..., M, in a quantitative competition method for a system in which said M participant devices send their aimed values to a server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps of:

(a-1) processing an initial value inherent to said participant device m with a predetermined one-way function by the number of times corresponding to said aimed value to generate aimed value information

$\gamma_m = g(h^{km}(IV_m))$

where g is a one-way function, IV_m is said initial value, k_m is an index corresponding to the aimed value of said participant device m and $h^{km}(IV_m)$ indicates processing of said initial value IV_m with a one-way function h by k_m times;

(a-2) generating verification information $C_m = h^{K+1}(IV_m)$ and sending said verification information to said server device together with said aimed value information γ_m;

(b) generating said initial value updated by the number of times requested by said server device and sending said updated initial value to said server device; and

(c) sending said aimed value information $\gamma_m = g(h^{km}(IV_m))$ to said server device.

50. The recording medium of claim 49, wherein said step (b) includes a step of generating $D_m = h^k(IV_m)$ as said updated initial value corresponding to said index k and sending said updated initial value to said server device in

response to its request.

51. A recording medium on which there is recorded as a program the procedure which is followed by an m-th one of M participant devices, where m = 1, 2, ..., M, in a quantitative competition method for a system in which said M participant devices send their aimed values to a server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps of:

(a-1) computing aimed value information by

$\gamma_m = g(h^{km}(IV_m))$

where g is a one-way function, IV_m is said initial value, k_m is an index corresponding to the aimed value PR_m of said participant device m and $h^{km}(IV_m)$ indicates processing of said initial value IV_m with a one-way function h by k_m times;

(a-2) generating verification information $C_m = h^{K+1}(IV_m)$;

(a-3) generating $h(PR_m(+)R_m)$ from a random number R_m and said aimed value PR_m and sending said $h(PR_m(+)R_m)$ to said server device together with said aimed value information γ_m and said verification information C_m, said (+) indicating a predetermined arbitrary operation;

(b-1) sending said aimed value PR_m and said random number R_m to said server device in response to its request; and

(b-2) generating $D_m = h^k(IV_m)$ as said updated initial value corresponding to said index k and sending said updated initial value to said server device in response to its request to present said $h^k(IV_m)$.

52. The recording medium of claim 51, wherein said step (a-3) is a step of generating $h(PR_m(+)R_m)$ from a random number R_m, said aimed value PR_m and additional information I_m about the sending of said aimed value information indicated by said participant device m and sending said $h(PR_m(+)R_m)$ to said server device, said additional information I_m being sent to said server device in said step (b-2).

53. A recording medium on which there is recorded as a program the procedure which is followed by an m-th one of M participant devices, where m = 1, 2, ..., M, in a quantitative competition method for a system in which said M participant devices send their aimed values to a server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps wherein:

(a) upon each processing of said initial value with said one-way function h, said each participant device generates an updated initial value by adding said processed initial value with select information $b_m^{(k)}$ indicating whether said processed initial value is an aimed value for one value of said index k, and generates $H_m^{(K)}$ by repeatedly performing this processing from at least that index k_m of a sequence of indexes which corresponds to said aimed value to the upper limit value K, and sends said $H_m^{(K)}$ as said aimed value information to said server device;

(b-1) said server device requests said each participant device to send an updated initial value $\{H_m^{(k-1)}, b_m^{(k)}\}$ corresponding to each value of said index k in descending order from K; and

(b-2) said each participant device generates and sends $\{H_m^{(k-1)}, b_m^{(k)}\}$ as said updated initial value to said server device.

54. A recording medium on which there is recorded as a program the procedure which is followed by an m-th one of M participant devices, where m = 1, 2, ..., M, in a quantitative competition method for a system in which said M participant devices send their aimed values to a server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps of:

(a) generating $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ as said aimed value information using a predetermined positive integer x_m, an initial value IV_m and one-way functions h and g, and sends said aimed value information to said server device;

(b-1) decides whether its received index k from said server device is the index k_m corresponding to said aimed value;

(b-2) if the result of decision in step (b-1) is $k = k_m$, generating and sending $H_m^{(k-1)} = g^{xm-1}(IV_m)$ as said updated initial value to said server device; and

(b-3) if the result of decision in said step (b-1) is not $k = k_m$, generating and sending $H_m^{(k-1)} = h^{k-km-1}(g^{xm}(IV_m))$ as said updated initial value to said server device.

55. A recording medium on which there is recorded as a program the procedure which is followed by an m-th one of M participant devices, where m = 1, 2, ..., M, in a quantitative competition method for a system in which

said M participant devices send their aimed values to a server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, letting the initial value of said each participant device be represented by IV_m, said procedure comprising the steps of:

(a) generating $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ as said aimed value information using a predetermined positive integer x_m, an initial value IV_m and one-way functions h and g, and sends said aimed value information to said server device;

(b-1) decides whether its received index k from said server device is the index k_m corresponding to said aimed value;

(b-2) if the result of decision in step (b-1) is $k = k_m$, generating $H_m^{(k-1)} = g^{xm-1}(IV_m)$ as said updated initial value and sending said updated initial value to said server device together with a flag indicating that said k and k_m are equal; and

(b-3) if the result of decision in said step (b-1) is not $k = k_m$, generating and sending $H_m^{(k-1)} = h^{k-km-1}(g^{xm}(IV_m))$ as said updated initial value to said server device.

56. A recording medium on which there is recorded as a program the procedure which is followed by an m-th one of M participant devices, where $m = 1, 2, \ldots, M$, in a quantitative competition method for a system in which said M participant devices send their aimed values to a server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received, and there is

provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the step of:

(a) processing, with a predetermined one-way function h and through the use of said conversion table, information $k(+)b_m^{(k)}(+)R_m^{(k)}$, which contains each index k equal to or larger than an index k_m corresponding to said aimed value, select information $b_m^{(k)}$ indicating whether said index k corresponds to said aimed value, and a random number $R_m^{(k)}$, to generate at least $K-k_m+1$ pieces of aimed value information $h(k(+)b_m^{(k)}(+)R_m^{(k)})$, and sends these pieces of aimed value information to said server device, A(+)B representing a predetermined arbitrary operation.

57. The recording medium of claim 56, wherein said procedure further comprises a step of sending to said server device a random number $R_m^{(k)}$ corresponding to the index k received from said server device.

58. The recording medium of claim 56, wherein said step (a) includes a step of sending a random number $R_m^{(k)}$ to said server device together with said $h(k(+)b_m^{(k)}(+)R_m^{(k)})$.

59. The recording medium of claim 49, 51, 53, 54, 55 or 56, wherein let an arbitrary aimed value be represented by PR = F(k)+Q, where F(k) is a value in said conversion table corresponding to said index k and Q is a fraction which is a positive integer which satisfies $F(k+1)-F(k)>Q\geq 0$;

said procedure further comprises a step wherein, letting said aimed value PR_m of said each participant device m be represented by $PR_m = F(k_m)+Q_m$, said each participant device m sends said fraction Q_m to said server device together with said aimed value information γ_m.

60. The recording medium of claim 49, 51, 53, 54, 55 or 56, wherein

said sequences of indexes k and values selectable as said aimed values are both monotonous increasing values in the same direction.

61. The recording medium of claim 49, 51, 53, 54, 55 or 56, wherein said sequences of indexes k and values selectable as said aimed values are both monotonous increasing values in opposite directions.

62. The recording medium of claim 49, 51, 53, 54, 55 or 56, wherein said procedure further comprises the steps of:

(0-1) sending the identifier ID_m of said each participant device to a provisional identifier registration device;

(0-2) receiving a provisional identifier AID_m from said provisional identifier registration device; and

(0-3) sending said provisional identifier AID_m as an identifier to said server device together with said aimed value information.

63. A recording medium on which there is recorded as a program the procedure which is followed by a server device in a quantitative competition method for a system in which a plurality of participant devices send their aimed values to said server device and said server device determines which of said participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps of:

(a) publishing aimed value information $\gamma_m = g(h^{km}(IV_m))$ received from said each participant device on a bulletin board accessible from all of said participant device, g being a one-way function, IV_m being said initial value, k_m being an index corresponding to the aimed value of said each participant

device m and $h^{km}(IV_m)$ indicating processing of said initial value IV_m with a one-way function h by k_m times;

(b) generating an updated initial value by $D_m = g(h^k(IV_m))$;

(c) checking whether there is any aimed value information γ_m which is equal to said updated initial value D_m; and

(d) upon first detection of a match in said step (c), deciding that the aimed value of the participant device corresponding to said updated initial value D_m which matches said aimed value information γ_m.

64. The recording medium of claim 63, wherein said step (a) includes a step of publishing verification information $C_m = h^{K+1}(IV_m)$ received from said each participant device on said bulletin board together with said aimed value information γ_m.

65. The recording medium of claim 64, wherein: said step (b) includes the steps of:

(b-1) requesting said each participant device to send $D_m = h^k(IV_m)$ corresponding to said index k; and

(b-2) receiving from said each participant device $D_m = h^k(IV_m)$ as said updated initial value corresponding to said index k; and

said step (c) includes a step of generating $g(D_m)$ and making a check for said aimed value information $\gamma_m = g(D_m)$.

66. The recording medium of claim 65, wherein:

said step (b) includes a step (b-0) of setting said index k to an upper limit value K; and

said step (c) includes the steps of:

(c-1) publishing said $D_m = h^k(IV_m)$ received from said each participant device on said bulletin board;

(c-2) computing said $g(D_m)$ for said each participant device m;

(c-3) making a check to see if said $g(D_m)$ matches said aimed value information;

(c-4) if no match is detect for any of said m in said step (c-3), replacing said D_m with said C_m, decrementing said index k by one and returning to said step (b-1); and

(c-5) if a match is detected in said step (c-3), determining that the value corresponding to said index k at that time is said maximum or minimum aimed value.

67. The recording medium of claim 66, wherein said step (c-1) includes a step of generating $h(D_m)$ and making a check to see if $h(D_m) = C_m$ holds.

68. The recording medium of claim 66, wherein said procedure includes a step of publishing said determined maximum or minimum aimed value and said $h^{km}(IV_m)$ on said bulletin board.

69. The recording medium of claim 63, wherein:

said step (b) includes the steps of

(b-0) setting said index k to an upper limit value K;

(b-1) inquiring said each participant device m about whether said aimed value information corresponds to said index;

(b-2) checking whether an answer from said each participant device acknowledges said correspondence;

(b-3) if said answer from said each participant device denies said correspondence, decrementing said k by one and returning to said step (b-1);

(b-4) if said answer from said each participant device acknowledges said correspondence, requesting said each participant device to present an updated initial value $h^k(IV_m)$;

(b-5) publishing $D_m = h^k(IV_m)$ from said each participant device on

said bulletin board; and

said step (c) includes the steps of:

(c-1) generating $h(D_m)$'s for all of said D_m's;

(c-2) checking whether said $h(D_m)$'s match said verification information C_m's on said bulletin board, respectively;

(c-3) if no mismatch is detected in said step (c-1), generating $g(D_j)$ for D_j presented by a participant device j having bid;

(c-4) checking whether said $g(D_j)$ matches said aimed value information γ_j of said participant device j on said bulletin board; and

(c-5) if said $g(D_j)$ matches said γ_j in said step (c-4), decides that said participant device j sent to said server device said aimed value information corresponding to said aimed value k.

70. The recording medium of claim 63, wherein:

said step (b) includes the steps of:

(b-1) publishing its received γ_m, $h(PR_m(+)R_m)$ and ID_m on said bulletin board, said (+) indicating a predetermined arbitrary operation;

(b-2) requesting said each participant device to present its aimed value PR_m and random number R_m;

(b-3) determining from its received PR_m and R_m an index k corresponding to the maximum one of said aimed values and a participant device j having sent said aimed value information corresponding to said index k;

(b-4) requesting all of said participant devices to present $h^k(IV_m)$; and

(b-5) receiving $D_m=h^k(IV_m)$ as said updated initial value from said each participant device;

said step (c) includes the steps of:

(c-1) publishing all of its received D_m's on said bulletin board;

(c-2) generating $h(D_m)$'s for all of said D_m's;

(c-3) checking whether said $h(D_m)$'s match said verification information C_m's on said bulletin board, respectively;

(c-4) if no mismatch is detected in said step (c-3), generating $g(D_j)$ for D_j presented by said participant device j having sent said maximum aimed value determined in said step (b-4); and

(c-5) checking whether said $g(D_j)$ matches said aimed value information γ_j of said participant device j on said bulletin board; and

said step (d) includes a step of deciding that said participant device j sent said aimed value information for said aimed value k, if a match is detected in said step (c-5).

71. The recording medium of claim 70, wherein said step (d) includes the steps of:

(d-1) generating $E_m = g(h^{t-k}(h^k(IV_m))$ for t such that $k \leq t \leq K$ and for all of said m's except said j;

(d-2) checking whether these E_m's match said aimed value information γ_m on said bulletin board; and

(d-3) if no match is detected in said step (d-2), deciding that said k is an index corresponding to the maximum or minimum aimed value, and outputting said k and said identifier ID_m of said participant device j having presented said aimed value.

72. The recording medium of claim 70 or 71, wherein

said step (b-2) includes a step of requesting all of said participant devices to present additional information I_m as well as said aimed value PR_m and said random number R_m.

73. A recording medium on which there is recorded as a program the procedure which is followed by a server device in a quantitative competition

method for a system in which a plurality of participant devices send their aimed values to said server device and said server device determines which of said participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps of:

(a) receiving, from each of participant devices, $h(H_m^{(K)})$ generated as aimed value information of said each participant device by repeating, for each of a sequence of index values k from at least k_m corresponding to an aimed value of said each participant device to an upper limit index value K, processing of:

combining an initial value of said each participant device with select information to provide combined information and

operating a one-way function h on said combined information to generate an updated value, said select information indicating whether said each index value k is an aimed value or not, and

publishing said aimed value information $h(H_m^{(K)})$ on a bulletin board accessible from all of said participant devices and any other devices as well;

(b) requesting said each participant device to send an updated initial value $\{H_m^{(k-1)}, b_m^{(k)}\}$ corresponding to each value of said index k in descending order from K;

(c) publishing said updated initial value $\{H_m^{(k-1)}, b_m^{(k)}\}$ on said bulletin board;

(d) processing said updated initial value $\{H_m^{(k-1)}, b_m^{(k)}\}$ with said one-way function h to generate $H_m^{(k)} = h(H_m^{(k-1)} || b_m^{(k)})$;

(e) checking whether said updated initial value $H_m^{(k)}$ matches $H_m^{(k)}$ in

$\{H_m^{(k)}, b_m^{(k+1)}\}$ received previously; and

(f) if a match is detected in said step (e), deciding whether said select information $b_m^{(k)}$ represents that the corresponding index k is the index k_m of said aimed value; and

(g) if the result of decision in said step (f) is true, outputting said index k concerned and the corresponding participant device number m, and if the result of decision is false, said server device returns to said step (b) and repeats processing for the next index value k.

74. A recording medium on which there is recorded as a program the procedure which is followed by a server device in a quantitative competition method for a system in which a plurality of participant devices send their aimed values to said server device and said server device determines which of said participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps wherein said server device:

(a) receives $H_m^{(K)}$ as said aimed value information from said each participant device which, upon each processing of said initial value with said one-way function h, generates an updated initial value by adding said processed initial value with select information $b_m^{(k)}$ indicating whether said processed initial value is an aimed value for one value of said index k, and generates $H_m^{(K)}$ by repeatedly performing this processing from at least that index k_m of a sequence of indexes which corresponds to said aimed value to the upper limit value K, and publishes said aimed value information $H_m^{(K)}$ on a bulletin board accessible from all of said participant device;

(b) for each value of said index k in order descending from K, inquires

said each participant device about whether it has bid for said index k, said each participant device responding YES or NO to said inquiry;

(c) upon first detection of the response YES, requests said each participant device to send its updated initial value $H_m^{(k-1)}$; and

(d) receives $H_m^{(k-1)} = h(H_m^{(k-2)} || b_m^{(k-1)})$ as said updated initial value from said each participant device and publishes said received updated initial value on said bulletin board;

(e) letting a and $\underline{a}$ represent predetermined values of said select information $b_m^{(k)}$ indicating bidding and not bidding, respectively, generates, for said participant device m having bid for the current index k,

$$H_m = h(\ldots h(h(H_m^{(k-1)} || a) || \underline{a}) \ldots || a)$$

through the use of said updated initial value $H_m^{(k-1)}$, and for every one of the other participant devices m, generates

$$H_m = h(\ldots h(h(H_m^{(k-1)} || \underline{a}) || \underline{a}) \ldots || a)$$

through the use of said updated initial values $H_m^{(k-1)}$;

(f) checks whether said H_m for said each participant device matches said $H_m^{(k)}$ published on said bulletin board; and

(g) if a match is detected in said step (f), determines that said participant device having responded YES is the winning bidding device, and publishes the current value of said index k as the index k_m of the aimed value of said winning bidding device.

75. A recording medium on which there is recorded as a program the procedure which is followed by a server device in a quantitative competition method for a system in which a plurality of participant devices send their aimed values to said server device and said server device determines which of said participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the

relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps of:

(a) letting the initial value of said each participant device be represented by IV_m, receiving from said each participant device $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ generated as said aimed value information using a predetermined positive integer x_m, said initial value IV_m and one-way functions h and g;

(b) publishing said aimed value information A_m on a bulletin board accessible from all of said participant devices; and

(c) sending said index k to said each participant device to ask for its updated initial value;

(d) processing said updated initial value $H_m^{(k-1)}$ with said one-way function h to generate $h(H_m^{(k-1)})$;

(e) deciding whether said $h(H_m^{(k-1)})$ is equal to said aimed value information $H_m^{(K)}$;

(f) if it is decided in said step (e) that they are equal, updating said aimed value information $H_m^{(K)}$ with said updated initial value $H_m^{(k-1)}$, then decrementing said index k by one and returning to said step (c);

(g) if it is decided in said step (e) that they are not equal, processing said updated initial value $H_m^{(k-1)}$ with said one-way function g to generate $g(H_m^{(k-1)})$; and

(h) deciding whether said $g(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$; and

(i) deciding that the aimed value of said participant device corresponding to m and k having provided said match is the maximum or minimum, if a match is detected in said step (h).

76. A recording medium on which there is recorded as a program the

procedure which is followed by a server device in a quantitative competition method for a system in which a plurality of participant devices send their aimed values to said server device and said server device determines which of said participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps wherein said server device:

(a), letting the initial value of said each participant device be represented by IV_m, where m = 1, 2, ..., M, M being an integer equal to or greater than 2, receives from each participant device, as said aimed value information, $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ using a predetermined positive integer x_m, said initial value IV_m and one-way functions h and g, and publishes said received aimed value information on a bulletin board accessible from all of said participant devices;

(b) for each value of said index k in order descending from K, inquires said each participant device about whether it has bid for said index k, said each participant device responding YES or NO to said inquiry;

(c) upon first detection of the response YES, requests said each participant device to send its updated initial value $H_m^{(k-1)}$;

(d) receives from said each participant device $H_m^{(k-1)} = g^{xm-1}(IV_m)$ if $k = k_m$ and $H_m^{(k-1)} = h^{k-km-1}(g^{xm}(IV_m))$ if $k \neq k_m$;

(e) for said updated initial value $H_m^{(k-1)}$ received from said participant device having responded YES, generates

$$H_m = h^{K-km}g(H_m^{(k-1)})$$

and for said updated initial value received from said each participant device having responded NO, generates

$H_m = h^{K+1-k}g(H_m^{(k-1)})$

(f) checks whether said H_m for said each participant device matches said $H_m^{(K)}$ published on said bulletin board; and

(g) if a match is detected in said step (f), determines that said participant device having responded YES is the winning bidding device, and publishes the current value of said index k as the index K_m of the aimed value of said winning bidding device.

77. A recording medium on which there is recorded as a program the procedure which is followed by a server device in a quantitative competition method for a system in which a plurality of participant devices send their aimed values to said server device and said server device determines which of said participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, said procedure comprising the steps of:

(a) letting the initial value of said each participant device be represented by IV_m, receiving from said each participant device $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ generated as said aimed value information using a predetermined positive integer x_m, said initial value IV_m and one-way functions h and g;

(b) publishing said aimed value information $H_m^{(K)}$ on a bulletin board accessible from all of said participant devices; and

(c) sending said index k to said each participant device to ask for its updated initial value;

(d) checking whether its received updated initial value $H_{k,m}$ is added with said flag;

(e) if it is decided in said step (d) that said flag is added, processing

said updated initial value $H_m^{(k-1)}$ with said one-way function g to generate $g(H_m^{(k-1)})$;

(f) deciding whether said $g(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$;

(g) if it is decided in said step (d) that no flag is added, processing said updated initial value $H_m^{(k-1)}$ with said one-way function h to generate $h(H_m^{(k-1)})$;

(h) deciding whether said $h(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$;

(i) if it is decided in said step that they are equal, updating said aimed value information $H_m^{(K)}$ with said initial value $H_m^{(k-1)}$, then decrementing said index k by one and returning to said step (c); and

(j) if it is decided in said step (h), processing said initial value $H_m^{(k-1)}$ with said one-way function g to generate $g(H_m^{(k-1)})$ and returning to said step (f); and

(k) if a match is detected in said step (f), deciding that the aimed value of said participant device corresponding to m and k having provided said match is the maximum or minimum.

78. A recording medium on which there is recorded as a program the procedure which is followed by a server device in a quantitative competition method for a system in which a plurality of participant devices send their aimed values to said server device and said server device determines which of said participant devices has offered the maximum or minimum one of said aimed values received, and there is provided a conversion table showing the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, and m = 1, 2, ..., M, M being an integer equal to or greater than 2;

said procedure comprising the steps of:

(a) receiving from each of said participant devices at least $K-k_m+1$ pieces of aimed value information $h(k(+)b_m^{(k)}(+)R_m^{(k)})$ generated by processing, with a predetermined one-way function h and through the use of said conversion table, information $k(+)b_m^{(k)}(+)R_m^{(k)}$, which contains each index k equal to or larger than an index k_m corresponding to said aimed value, select information $b_m^{(k)}$ indicating whether said index k corresponds to said aimed value, and a random number $R_m^{(k)}$, A(+)B representing a predetermined arbitrary operation between A and B;

(b) receiving and publishing said aimed value information on a bulletin board accessible from all of said participant devices;

(c) obtaining said random number R_m corresponding to each of said sequence of indexes k;

(d) calculating $h(k(+)a(+)R_m^{(k)})$, where a is a predetermined value with which said select information $b_m^{(k)}$ indicates said aimed value;

(e) checking said aimed values on said bulletin board for matching with said calculated $h(k(+)a(+)R_m^{(k)})$; and

(f) if a match is detected in said step (e), deciding that the aimed value of the aimed value information of a participant device having sent said random number $R_m^{(k)}$ at that time is the maximum or minimum value.

79. The recording medium of claim 78, wherein said procedure further comprises a step of repeating said steps (c), (d) and (e) if a match is detected in said step (d).

80. The recording medium of claim 79, wherein said step (c) includes the steps of: requesting said each participant device to send said random number $R_m^{(k)}$ corresponding to said index k; and receiving said random number $R_m^{(k)}$ from said each participant device.

81. The recording medium of claim 79, wherein:

said step (a) includes a step of receiving said random number $R_m^{(k)}$ sent from said each participant device together with said aimed value information $h(k(+)b_m^{(k)}(+)R_m^{(k)})$;

said step (b) includes a step of storing said random number $R_m^{(k)}$ in a nonpublic memory; and

said step (c) includes the steps of: requesting said each participant device to send said random number $R_m^{(k)}$ corresponding to said index k; and receiving said random number $R_m^{(k)}$ from said each participant device.

82. The recording medium of claim 63, 64, 69, 70, 73, 74, 75, 76, 77 or 78, wherein said sequences of indexes k and values selectable as said aimed values are both monotonous increasing values in the same direction, and in said step (c) said server device determines the maximum aimed value.

83. The recording medium of claim 63, 64, 69, 70, 73, 74, 75, 76, 77 or 78, wherein said sequences of indexes k and values selectable as said aimed values are both monotonous increasing values in opposite directions, and in said step (c) said server device determines the minimum aimed value.

84. The recording medium of claim 63, 64, 69, 70, 73, 74, 75, 76, 77 or 78, wherein let an arbitrary aimed value be represented by $PR = F(k)+Q$, where F(k) is a value in said conversion table corresponding to said index k and Q is a fraction which is a positive integer which satisfies $F(k+1)-F(k)>Q\geq 0$;

said step (a) includes a step wherein, letting said aimed value PR_m of said each participant device m be represented by $PR_m = F(k_m)+Q_m$, said server device receives from each participant device m said aimed value information generated by processing said initial value with said one-way function h by the number of times corresponding to k_m, together with said fraction Q_m, where m

= 1, 2, ..., M, said M being an integer equal to or greater than 2, and said server device publishes said aimed value information and said fraction Q_m on a bulletin board accessible from all of said participant devices;

said step (c) includes a step where said server device makes a check for matching between said updated initial value and said aimed value information for each index value in an ascending or descending order of said fraction Q_m where m = 1, 2, ..., M; and

said step (d) includes a step wherein, upon first detection of a match in said step (c), said server device finishes said check and determines, from k_m and m at the time of detecting the match, that $PR_m = F(k_m)+Q_m$ is said maximum or minimum aimed value.

85. The recording medium of claim 78 or 79, wherein let an arbitrary aimed value be represented by PR = F(k)+Q, where F(k) is a value in said conversion table corresponding to said index k and Q is a fraction which is a positive integer which satisfies $F(k+1)-F(k)>Q\geq 0$;

said step (a) includes a step wherein, letting said aimed value PR_m of said each participant device m be represented by $PR_m = F(k_m)+Q_m$, said server device receives said fraction Q_m together with said aimed value information;

said step (b) includes a step of publishing said fraction Q_m on said bulletin board together with said aimed value information, where m = 1, 2, ..., M, said M being an integer equal to or greater than 2;

said step (e) includes a step of making said check for matching for each index value in an ascending or descending order of said fraction Q_m where m = 1, 2, ..., M; and

said step (f) includes a step wherein, upon first detection of a match in said step (c), said server device finishes said check and determines, from k_m and m at the time of detecting the match, that $PR_m = F(k_m)+Q_m$ is said

maximum or minimum aimed value.

86. A quantitative competition system which comprises a server device and M participant devices each connected via a communication channel to said server device and in which said M participant devices send their aimed values to said server device and said server device determines which of said M participant devices has offered the maximum or minimum one of said aimed values received,

each of said participant devices comprising:

aimed value generating means for generating an aimed value PR_m;

aimed value transforming means provided with a conversion table memory having stored therein a conversion table which defines the relationships between a sequence of values selectable as said aimed values and a sequence of indexes corresponding thereto, for converting said aimed value PR_m to the corresponding index k_m and which processes said aimed value with a predetermined one-way function by the number of times corresponding to said aimed value to obtain aimed value information; and

sending means for sending to said server device said aimed value information and an identifier identifying said participant device; and

said server device comprising:

a conversion table memory which has stored therein a conversion table which is the same as said conversion table;

a bulletin board on which said server device writes said aimed value information an identifier received from said each participant device;

updated initial value acquiring means which acquires an updated initial value obtained by processing said initial value with a one-way function repeatedly in correspondence with values of an index k which is a

predetermined consecutive positive integers;

a counter which updates said index k one by one; and

control means which, upon each updating of said index k, compares said updated initial value with said aimed value information on said bulletin board to check whether they match, and determines m and k at the time of first detection of a match.

87. The system of claim 86, wherein said each participant device has initial value updating means for processing said initial value with a one0way function h to generate an updated initial value and for sending said updated initial value to said server device, and said updated initial value acquiring means of said server device receives said updated initial value from said each participant device.

88. The system of claim 86, wherein said updated initial value acquiring means of said server device processes said initial value with a one-way function h to generate said updated initial value.

89. The system of claim 87 or 88, wherein said aimed value transformer of said each participant device comprises:

a one-way function h processor which processes an initial value IV_m inherent to said participant device with a one-way function h by the number of times corresponding to said index k_m to obtain an output $h^{km}(IV_m)$; and

a one-way function g processor which processes said output from said one-way function h processor with a one-way function g to obtain said aimed value information.

90. The system of claim 89, wherein said aimed value transformer of said each participant device includes verification information generating means for processing said initial value IV_m with said one-way function h by K+1 times to generate $C_m = h^{K+1}(IV_m)$ as verification information and for

sending said verification information to said server device;

wherein there is published on said bulletin board $C_m = h^{K+1}(IV_m)$ received from said each participant device in advance, said server device further comprising a one-way function h processor which processes said response D_m with a one-way function h to generate $h(D_m)$, and

wherein said control means checks whether $C_m = h(D_m)$ holds, and if not, rewrites said C_m with said D_m and updates said index k on said counter.

91. The system of claim 86, wherein said each participant device comprises:

a random generator for generating a random number R_m;

an operating device for operating said random number R_m and said aimed value PR_m to obtain $PR_m(+)R_m$, where (+) represents a predetermined arbitrary operation;

one-way function h processing means for processing said $PR_m(+)R_m$ with a one-way function h to obtain $h(PR_m(+)R_m)$; and

verification information generating means for processing said initial value IV_m with said one-way function h K+1 times to generate $C_m = h^{K+1}(IV_m)$; and wherein:

said $h(PR_m(+)R_m)$ and said verification information are sent to said server device together with said aimed value information;

in said server device:

there are published on said bulletin board $C_m = h^{K+1}(IV_m)$, said aimed value information $\gamma_m = h^k(IV_m)$ and $h(PR_m(+)R_m)$ received from said each participant device, said PR_m and said R_m being an aimed value and a random number of said each participant device m;

said control means decides the maximum or minimum aimed value from said aimed values PR_m and said random numbers R_m received from said

participant devices, and determines the index k_{mx} corresponding to said maximum or minimum aimed value and requests said each participant device to send $(D_m) = h^{kmx}(IV_m)$ corresponding to said index k_{mx};

said updated initial value acquiring means comprises a one-way function h processor for processing D_m with a one-way function h to generate $h^{K+1-kmx}(D_m)$, and a one-way function g processor for processing D_j with a one-way function g to generate $g(D_j)$; and

said control means makes a check to see if said $h^{K+1-kmx}(D_m)$ matches C_m on said bulletin board and if said $g(D_j)$ matches said γ_m on said bulleting board.

92. The system of claim 86, wherein said aimed value transformer of said each participant device comprises:

a conversion table memory which has stored therein a conversion table which defines indexes k = 1, 2, ..., K corresponding to K kinds of values selectable as aimed values;

a select information generator which generates select information $b_m^{(k)}$ indicating whether to select an aimed value corresponding to each of said indexes k = 1, 2, ..., K;

a random generator which generates a random number $R_m^{(k)}$ inherent to said participant device m and said index k;

an operating device which receives said index k, said random number $R_m^{(k)}$ and said select information $b_m^{(k)}$ and performs an operation $k(+)b_m^{(k)}(+)R_m^{(k)}$;

a one-way function h processor which processes said $k(+)b_m^{(k)}(+)R_m^{(k)}$ with a one-way function h to obtain $h(k(+)b_m^{(k)}(+)R_m^{(k)})$; and

a control device which computes said $h(k(+)b_m^{(k)}(+)R_m^{(k)})$ for each of said indexes k and provides the k pieces information as said aimed value

information;

in said server device:

there are published on said bulletin board $h(k(+)b_m^{(k)}(+)R_m^{(k)})$ together with said aimed value information γ_m received from said each participant device;

said server device further comprises an operator for operating $k(+)b(+)R_m^{(k)}$; and

a one-way function h processor for processing the result of said operation with a one-way function h to generate $h(k(+)b(+)R_m^{(k)})$, where b is a predetermined value which indicates that said select information $b_m^{(k)}$ has selected the aimed value corresponding to said index k; and

said control means makes a check for matching between said $h(k(+)b(+)R_m^{(k)})$ and said $h(k(+)b_m^{(k)}(+)R_m^{(k)})$ on said bulletin board.

93. The system of claim 86, wherein said aimed value transformer of said each participant device comprises:

a conversion table memory which has stored therein a conversion table which defines indexes k = 1, 2, ..., K corresponding to K kinds of values selectable as aimed values, for converting said aimed value PR_m to the corresponding index k_m;

initial value updating means which, for each index k, processes an initial value with a one-way function h and adds the processed initial value with select information $b_m^{(k)}$ for said index k to obtain an updated initial value and repeats this processing until k = K is reached, thereby generating $H_m^{(K)}$;

a one-way function h processor for outputting said updated initial value $H_m^{(k)}$ from said initial value updating means as said aimed value information;

select information generator which generates said select information

$b_m^{(k)}$ whether said aimed value corresponds to each index k from at least k_m to K;

a concatenator which concatenates said $H_m^{(k-1)}$ from said one-way function h processor and said select information $b_m^{(k)}$ to generate $H_m^k = h(H_m^{(k-1)}||b_m^{(k)})$;

a buffer which temporarily holds the output from said concatenator and outputs said output for the next value of said index k;

a storage part which, for each value of said index k, stores $H_m^{(k)}$ corresponding thereto; and

a second one-way function h processor by which $H_m^{(k)}$, obtained by repeating processing until k = K, is processed with a one-way function h to generate $h(H_m^{(k)})$, said $h(H_m^{(k)})$ being output as said aimed value information;

wherein said sending means is a means which responds to a request of said server device for said index k to read out $H_m^{(k)}$ from said storage part and send said $H_m^{(k)}$ to said server device;

in said server device:

there are published on said bulletin board, as said aimed value information, $h(H_m^{(k)})$ obtained by processing, with a one-way function h, $H_m^{(k)}$ generated by said each participant device which, upon each processing of said initial value with a one-way function h, added the processed value with select information $b_m^{(k)}$ indicating whether said value was an aimed value for each value of said index k and repeated this processing from at least the index k_m corresponding to said aimed value to the upper limit value K of said index k;

said initial value updating means includes a one-way function h processor by which $\{H_m^{(k-1)}, b_m\}$ received from said each participant device in answer to an inquiry for said index k is processed with a one-y function h to generate $H_m^{(k)} = h(H_m^{(k-1)}|| b_m^{(k)})$; and

said server device includes an updated initial value comparator for making a check to see if said $H_m^{(k)}$ matches $H_m^{(k)}$ in $\{H_m^{(k)}, b_m^{(k+1)}\}$ previously received.

94. The system of claim 86, wherein said aimed value transformer of said each participant device comprises:

a conversion table memory which has stored therein a conversion table which defines indexes k = 1, 2, ..., K corresponding to K kinds of values selectable as aimed values, for converting said aimed value PR_m to the corresponding index k_m;

a one-way function g processor which processes said initial value IV_m with a one-way function g by a predetermined number of times x_m to generate $g^{xm}(IV_m)$;

a one-way function h processor which processes said $g^{xm}(IV_m)$ with a one-way function h K-k_m times to generate $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ as said aimed value information; and

response generating means which responds to a request from said server device for k to decide whether $k=k_m$, and if true, generates $H_m^{(k-1)} = h^{k-km-1}(g^{xm}(IV_m))$, and if false, generates $H_m^{(k-1)} = g^{xm-1}(IV_m)$; and

wherein said sending means sends said $H_m^{(k-1)}$ in response to said request from said server device for said k; and

in said server device:

there is published on said bulletin board $H_m^{(K)} = h^{K-km}(g^{xm}(IV_m))$ as said aimed value information received from said each participant device, which further comprises a one-way function h processor by which $H_m^{(k-1)}$ received from said each participant device as an answer to an inquiry for said k is processed with a one-way function h to generate $h(H_m^{(k-1)})$, and a one-way function g processor for processing said answer $H_m^{(k-1)}$ with a one-way

function g to generate $g(H_m^{(k-1)})$; and

said control means: makes a check to see if said $h(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$ published on said bulletin board; if a match is detected, updates said aimed value information $H_m^{(K)}$ with said $H_m^{(k-1)}$ and decrements said index k on said counter by one; and if a mismatch is detected, makes a check to see if said $g(H_m^{(k-1)})$ matches said aimed value information $H_m^{(K)}$; and if a match is detected, determines, based on k and m at that time, the maximum or minimum aimed value PR_m and the participant device m having offered said value PR_m.

95. The system of claim 86, 87, 88, 91, 92, 93 or 94, wherein said aimed value transformer of said each participant device comprises;

a conversion table memory which has stored therein a conversion table which defines the relationships between a sequence of values selectable as said aimed values and a sequence of indexes k of integral values respectively corresponding thereto, for converting said aimed value PR_m to the corresponding index k_m;

a fraction calculating part which, letting an arbitrary aimed value PR be represented by $PR = F(k)+Q$, where F(k) is a value in said conversion table corresponding to said k and Q is a fraction which is a positive integer which satisfies $F(k+1)-F(k)>Q\geq 0$, calculates said fraction $Q_m = PR_m-F(k_m)$ based on $F(k_m)$ obtained from said conversion table and said aimed value PR_m; and

a one-way function h processor which processes said initial value IV_m with said one-way function h by the number of times corresponding to said k_m to generate said aimed value information; and

wherein said sending means sends said fraction Q_m to said server device together with said aimed value information; and

in said server device:

there is published on said bulletin board said fraction Q_m received from said each participant device together with said aimed value information; and said server device comprises:

a sequencer for deciding the sequence of said fractions Q_m on said bulletin board; and

select information comparator for checking whether said select information $b_m^{(k)}$ is equal to a value b indicating the selection of the aimed value corresponding to said index k in said decided sequence of fractions Q_m.

96. The system of claims 86, 87, 88, 91, 92, 93 or 94, wherein said sequence of index values k and said sequence of values selectable as said aimed values on said conversion table are monotone increasing values in the same direction, and said server device determines the maximum aimed value.

97. The system of claims 86, 87, 88, 91, 92, 93 or 94, wherein said sequence of index values k and said sequence of values selectable as said aimed values on said conversion table are monotone increasing values in opposite directions, and said server device determines the minimum aimed value.